ALGEBRA:

$$(X, \bullet, \times, *)$$

X – nosná množina

$\bullet, \times, *$ – operace

KAŽDÁ MÁ ARITU:

$(2, 1, 0)$

$$\bullet : \underline{X \times X} \to X$$

$$\times : X \to X$$

$$* : \quad \to X$$

$(\mathbb{N}, +, *)$ je algebra typu $(2, 2)$

$(RV, +, *)$ $(2, 1)$

$(\mathrm{int}_{64}, +, *, \&, |, \neg)$ $(2, 2, 2, 2, 1)$

VLASTNOSTI OPERACÍ

- asociativita

$(X, \cdot)$

- je asociativní $\Leftrightarrow \forall x, y, z \in X: \quad (x \cdot y) \cdot z = \cancel{z \cdot (y \cdot x)}$ $x \cdot (y \cdot z)$

$(\{a, b, c\}, \cdot)$

$\cdot$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

- je asociativní

$x \cdot (\_ \cdot \_) = (x \cdot \_) \cdot \_ = x$

$\cdot$	a	b	c
a	b	c	c
b	b	b	c
c	b	b	a

Protipříklad:

$a \cdot (b \cdot c) = a \cdot c = c$

$(a \cdot b) \cdot c = c \cdot c = a$

$a \neq c$

$(\mathbb{Z}, +)$

$(2^{\{a,b,c\}}, \cup)$ } asociativní

$(\mathbb{R}\setminus\{0\}, \%)$ – není asociativní

$$10/(5/2) = 10/2{,}5 = 4$$
$$\neq$$
$$(10/5)/2 = 2/2 = 1$$

$\boxed{\text{KOMUTATIVITA}}$

$(X, \cdot)$ je komutativní $\overset{def}{\iff} \forall x,y \in X: \; x \cdot y = y \cdot x$

$(\mathbb{Z}, +), (2^{\{a,b,c\}}, \cup)$ - jsou komutativní

$(\mathbb{R}\setminus\{0\}, \%)$ – není komutativní

Neutrální prvek

$(X, \cdot)$ n je neutrální prvek vzhledem k $\cdot$

$$\overset{def}{\iff} \forall x \in X : n \cdot x = x = x \cdot n$$

0 je neutrální pro $(\mathbb{Z}, +)$

1 $(\mathbb{Z}, *)$

„ε" $(RV, \cdot)$

Dk. že neutrální prvek je maximálně jeden.

Sporem: Předpokládejme, že existují $n_1, n_2 \in X$. $n_1 \neq n_2$ a oba jsou neutrální

$$\underbrace{n_1 = \overbrace{n_1 \cdot n_2}^{n_1 \text{ je neutrální}}}_{n_2 \text{ je neutrální prvek}} = n_2$$

SPOR S PŘEDPOKLADEM

$\boxed{\text{Inversní prvky}}$

$(X, \cdot)$ s neutrálním prvkem n

Algebra má inv. prvky vzhledem k $\cdot$

$\Leftrightarrow \boxed{\forall x \in X\ \exists x' \in X :\ x \cdot x' = n = x' \cdot x}$

Příklad $(\mathbb{Z}, +)$ $inv(x) = -x$

$(\mathbb{N}, +)$ $inv(x)$ neexistuje

$(\text{unsigned Int}, +)$ $inv(x) = \underline{maxint} - x + 1$

---

dk. že pro asociativní operaci s neutrálním prvkem 0 existuje vždy maximální 1 inversní prvek.

$\boxed{\text{SPOREM}}$ Nechť $x \in X$ a $x', x'' \in X$ jsou inversní prvky k x.

$$(x' \cdot x) \cdot x'' = x' \cdot (\underline{x \cdot x''})$$

$$0 \cdot x'' = x' \cdot 0$$

$$x'' = x'$$

GRUPA

$(A, \cdot)$ je grupa

1) $\cdot$ je asociativní
2) $(A, \cdot)$ má neutrální prvek $0 \in A$
3) $(A, \cdot)$ má inversní prvky

Někdy se uvádí
$(A, \cdot, 0, {}^{-1})$ typu $(2, 0, 1)$

$(\mathbb{Z}, +)$ je grupa

$(\mathbb{Z}, *)$
- $*$ je operace
- $*$ je asociativní
- $*$ má neutrální prvek 1
- $*$ nemá inv. prvky

$\Rightarrow$ $(\mathbb{Z}, *)$ není grupa

~~$(\mathbb{R}, *)$~~ je grupa
$(\mathbb{R} \setminus \{0\}, *)$

$(\Sigma^*, \cdot)$
- $\cdot$ je operace
- $\cdot$ je asociativní
- $\cdot$ ε je neutrální prvek

- ~~není asociativní~~ nemá inv. prvky protože $\cdot$ je „prodlužující" a z řetězce délky n>0 nelze získat „ε"

$(A, \circ)$ $\qquad A = \{a, b, c\}$

$\circ$	a	b	c
a	a	a	a
b	b	b	b
c	c	c	c

$\circ$ je asociativní
$\circ$ nemá neutrální prvek
$\Rightarrow$ NENÍ TO GRUPA

$$X = \left\{ \begin{pmatrix} a & b & 0 \\ c & d & 0 \\ x & y & 1 \end{pmatrix} \middle| \; a, b, c, d, x, y \in \mathbb{R} \right\}$$

mějme algebru $(X, \cdot)$ kde $\cdot$ je násobení matic

je to grupa?

- je to operace

$\Rightarrow$ je algebra

$$\begin{pmatrix} a_1 & b_1 & 0 \\ c_1 & d_1 & 0 \\ x_1 & y_1 & 1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 & 0 \\ c_2 & d_2 & 0 \\ x_2 & y_2 & 1 \end{pmatrix} = \begin{pmatrix} a_1 a_2 + b_1 c_2 & a_1 b_2 + b_1 d_2 & 0 \\ c_1 a_2 + d_1 d_2 & c_1 b_2 + d_1 d_2 & 0 \\ x_1 a_2 + y_1 c_2 + x_2 & b_2 x_1 + d_2 y_1 + y_2 & 1 \end{pmatrix}$$

neutrální prvek: $\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \in X$

asociativita:

Násobení matic je asociativní (pokud je definováno)

$$A\cdot(B\cdot C) = (A\cdot B)\cdot C$$

Inversní prvky:

pro matice tvaru

$$\begin{pmatrix} a & b & 0 \\ c & d & 0 \\ x & y & 1 \end{pmatrix} \quad \text{kde} \quad \underbrace{\begin{vmatrix} a & b \\ c & d \end{vmatrix}}_{\text{determinant}} = a\cdot d - b\cdot c \neq 0$$

je definována inversní matice.

NAZÝVAJÍ SE REGULÁRNÍ MATICE

ZÁVĚR Pokud X je množina matic transformací pro které existuje inverse (regulární matice) pak $(X, \cdot)$ je grupa

OKRUH

algebra se 2 operacemi

$(A,+,0,-1,\cdot)$ je okruh pokud

- $(A,+,0,-1)$ je komutativní grupa
- $(A,\cdot)$: $\cdot$ je asociativní

$(A,+,0,-1,\cdot)$ komutativní okruh pokud $\cdot$ je komutativní

okruh s neutrálním prvkem $(A,+,0,-1,\cdot,1)$

1 je neutrální prvek operace $\cdot$

KOMUTATIVNÍ OKRUH S JEDN. PRVKEM $(A,+,0,-1,\cdot,1)$

OBOR INTEGRITY pokud $0 \neq 1$

Příklad:

$(\mathbb{R},+,\cdot)$ je obor integrity

$(\mathbb{Z},+,\cdot)$ — " —

$\boxed{\text{KONGRUENCE}}$

$(X, \cdot)$ typu (2)

relace $\sim$ je kongruence $\Leftrightarrow$

- $\sim$ je relace ekvivalence (symetrická, reflexivní, transitivní)
- $\forall x_1, x_2, x_3, x_4 \in X: \quad x_1 \sim x_2 \wedge x_3 \sim x_4 \Rightarrow (x_1 \cdot x_3) \sim (x_2 \cdot x_4)$

Příklad:

$(\mathbb{N}, +)$

ekvivalenční třídy $\{0\}, \{1\}, \{2\}, \langle 3, \infty)$

$\sim = \{(0,0), (1,1), (2,2)\} \cup \{(i,j) \mid i,j \geq 3\}$

je to kongruence?

$[0]_\sim + [0]_\sim = [0]_\sim \qquad [0]_\sim + [1]_\sim = [1]_\sim \qquad [0]_\sim + [2]_\sim = [2]_\sim$

$[1]_\sim + [1]_\sim = [2]_\sim \qquad \dots$

- $(\mathbb{N}/\sim, +)$ je $\boxed{\text{faktorová algebra}}$ $\quad N/\sim = \{[0]_\sim, [1]_\sim, [2]_\sim, [3]_\sim\}$

$(\mathbb{N}, +)$

$\sim = \{ (2i, 2i), (2i, 2i+1), (2i+1, 2i), (2i+1, 2i+1) \mid i \in \mathbb{N} \}$

Rozklad:

$\{0,1\}, \{2,3\}, \{4,5\}, \{6,7\}, \ldots$

Je to kongruence?

$0 \sim 1 \wedge 0 \sim 1 \Rightarrow 0+0 \sim 1+1 \Rightarrow \underline{0 \sim 2}$

$\underline{\text{SPOR}}$

$\Rightarrow$ <u>NENÍ KONGRUENCE</u>

ZBYTKOVÉ TŘÍDY „k"

$$\sim_k = \{ (i,j) \mid i \bmod k = j \bmod k \}$$

ČASTO SE ZNAČÍ $\equiv_k$

- je kongruence vzhledem k $+, \cdot,$

$(\mathbb{N}, +, \cdot)$

Rozklad

$(\mathbb{N}/\equiv_k, +, \cdot)$ faktorová algebra s $\mathbb{N}/\equiv_k = \{ [0]_{\equiv_k}, [1]_{\equiv_k}, \dots, [k-1]_{\equiv_k} \}$

HOMOMORFISMUS

$(A, \cdot)$ $(B, *)$ jsou algebry typu 2

$\boxed{h: A \to B}$ je homomorfismus

- zobrazení z A do B (každému prvku z A přiřazujeme prvek z B)

- zachovává výsledky operací

$\forall x_1, x_2 \in A$ $h(x_1) * h(x_2) = h(x_1 \cdot x_2)$

Příklad $(\mathbb{Z}, +)$ $(\mathbb{Z}_3, +)$

$h: \mathbb{Z} \to \mathbb{Z}_3$ definována $h(x) = x \bmod 3$

je homomorfismus

$(\mathbb{Z}, +)$ $(\{0,1\}, \oplus)$

$\oplus$	0	1
0	0	1
1	1	1

Nechť

$$h(i) = \begin{cases} 0 & \text{pro } i = 0 \\ 1 & \text{pro } i \neq 0 \end{cases}$$

Pokud je h homomorfismus, tak

musí platit pro $x_1 = 1$ a $x_2 = -1$

$$h(1) \oplus h(-1) = h(1-1)$$

$$1 \oplus 1 = h(0)$$

$$1 = 0$$

SPOR $\Rightarrow$ h homomorfismus není

Pro $(\mathbb{N}, +)$ je h homomorfismus

$(\mathbb{R}, +)$ $(\mathbb{Z}, +)$

zaokrouhlování je zobrazení z $\mathbb{R} \to \mathbb{Z}$

$$\text{round}(a+b) = \text{round}(a) + \text{round}(b)$$

$$\text{round}(1{,}4+1{,}4) = \text{round}(1{,}4) + \text{round}(1{,}4)$$

$$3 = 1 + 1$$

NEPLATÍ

$\Rightarrow$ round není homomorfismus

$(RV, \cdot, +, *)$ — reg. výrazy

$(\mathcal{L}_3, \cdot, \cup, *)$ — jazyky typu 3

$(\mathcal{A}, \cdot, \cup, *)$ — automaty

KLASICKÉ PŘEVODY JSOU homomorfismy